Plaintiffs Thomas Roger White, Jr. and Patricia Cauley, on behalf of themselves and all others similarly situated, allege the following against Defendants Samsung Electronics America, Inc. ("Samsung") and Sony Electronics Inc. ("Sony") (collectively, "Defendants") in this Second Amended Complaint:

I. INTRODUCTION AND SUMMARY OF CASE

1. If you plan a movie-night on your Samsung or Sony Smart TV, the privacy of your home will have a surprisingly *public* audience. In fact, while using your Smart TV to watch videos, engage "apps," or use other "smart" TV-features, your basic personal, private information (including your video line-up, who and where you are, and even the contents of your conversations) - will become a *public* affair. This is because Defendants' Smart TVs watch and record what you're watching, while you're watching it - and listen to and record what you're speaking, while you're speaking it.[1]

2. Defendants have violated the federal and state privacy rights of its consumers by failing to obtain "informed consent" and deceptively and unreasonably intercepting, storing, and unilaterally disclosing to third parties consumers' "digital identities;" namely, consumers' private information, sensitive viewing histories, personal preferences, contents of conversations, and other critical information particularly useful to uniquely identify individuals and their location. Such private information wrongfully disclosed by Defendants also includes, but is not limited to, the online services a consumer visited and the presence of a consumer's other Internet-connected devices. [2]

---

[1] Samsung's "Always-On" Voice Recorders
When the voice recognition feature on a Samsung Smart TV is enabled, everything a user says in front of the Samsung Smart TV is recorded and transmitted over the internet to a third party regardless of whether it is related to the provision of the service. See https://epic.org/privacy/internet/ftc/samsung/

[2] These are the exact concerns recently expressed by Senators Edward J. Markey of Massachusetts and Richard Blumenthal of Connecticut in a Letter dated July 12, 2018, to the Honorable Joseph Simons, Chairman of the Federal Trade Commission ("FTC") wherein they have asked that the FTC investigate the business practices of smart-television manufacturers amid worries that companies are tracking consumers' viewing behavior without informed consent. See Exhibit 1 (attached hereto). The Senators explicitly state that "*Smart TV users may not be aware of the extent to which their televisions are collecting sensitive information about their viewing habits . . . [and the Smart TV manufacturers] do[] not provide sufficient information about its privacy practices to ensure users can make truly informed decisions*." Id. (emphasis added).

3. Defendants also secretly collect and disclose to third parties consumers' Internet Protocol (IP) addresses, media access control (MAC) addresses, and zip codes. In this advanced technological-age, this data and other personally identifiable information disclosed by Defendants to third parties can easily be used by an ordinary person to pinpoint a consumer's physical location (i.e., "geolocation" information) and electronic identity.

4. Defendants accomplish their massive data-mining enterprise through their use of invasive Automatic Content Software ("ACS") - that is secretly installed by Defendants on millions of their Smart TVs (including Plaintiffs' Smart TVs at issue). Defendants then unilaterally disclose consumers' personally-identifiable information and other consumer-data to advertisers and media content providers (in addition to other third parties, such as data processors), who in turn deliver targeted advertisements to unsuspecting consumers across their devices.

5. Targeted ads are sent not just to the Smart TVs themselves, but also to any smartphones, tablets, PCs, or other devices within the home that share the same Internet connection as Defendants' Smart TV.

6. Monetizing consumer data is a critical part of Defendants' business plan because, due to fierce market competition, Defendants reap extremely *slim* profit margins on TV sales. To offset this, Defendants have engaged in the illegal *industry-standard*, described herein, to deceptively utilize ACS technology and profit from their unfair collection and disclosure to third parties of a rich portfolio of "siphoned" consumer data and information.

7. In essence, Defendants' business plan treats all consumers as Defendants' very own Nielsen family. The critical difference is that, unlike Defendants' Smart TV consumers, Nielsen family members *agree* to share their viewing habits and are paid for their participation.[3]

[3] In addition, Nielsen emphasizes to its customers that: "The information from your home is held strictly confidential. You will never be approached by anyone selling something because you participated in one of our surveys." https://www.nielsen.com/us/en/about-us/nielsen-families.html

8. By sharp contrast, Defendants' personal data and voice-recording collection and transmission using their hidden ACS technology is, ***by intention***, unbeknownst to consumers. And because of that fact, there could be no informed consent in this case. See infra.

9. Nowhere on its Smart TV box, or anywhere in its packaging (including the boxes and packaging related to Plaintiffs' Smart TVs at issue) do Defendants inform consumers that Defendants' collect and store indefinitely consumers' viewing histories and other personally identifiable information, or that Defendants sell consumers' private, personal information and contents of conversations to third parties, or that third-parties will respond with targeted ads across devices. Neither do Defendants disclose this material information in their own advertising and/or marketing.

10. Even though it would be simple and no-cost for Defendants to conspicuously alert consumers about their collections and sale of private consumer information: (i) on the television box itself (*ie*; prior to the purchase of the TV by the consumer); and/or (ii) in the instruction manual in the box; and/or (iii) on a conspicuous, separate and bold *"Privacy Information Sheet"* in the box -- Defendants choose not to do.[4]

11. Plaintiffs are consumers of Defendants' Smart TVs who did not consent to Defendants' invasive data-collection program. They bring this putative class action suit against Defendants to enforce their and other Samsung and Sony Smart TV-owners' privacy and consumer rights under federal and state law.[5]

12. In addition, Defendants' collection of consumers' private data and conversations and also their material omissions and misrepresentations regarding its data collection policies and invasive tracking software are deceptive, unfair, and misleading in

[4] Consider Defendants' representations in product packaging. While the packaging on Defendants' Smart TVs describe its features and indicate that the televisions are equipped to deliver video content through the Internet and can display content from cable and satellite providers, streaming devices, and other connected media sources, the packaging fails to inform (let alone adequately inform) consumers that if they take advantage of the TV's connectivity platform, their viewing data and other personal information will be collected and shared with others.

[5] On March 7, 2017, WikiLeaks first reported that Samsung Smart TVs were in fact being used by outside parties to spy on consumers' private-conversations, even when the device was supposedly turned "off."

violation of state consumer protection laws. Had Plaintiffs known the truth about Defendants' data collection practices and tracking software, they would not have purchased Defendants' Smart TVs or would have paid substantially less for them.

13. As described herein, Defendants representations were not sufficiently clear or prominent to alert consumers that Defendants engage in second-by-second tracking and recording of consumers using their ACS technology, and/or that Defendants sell consumers' private data and personal information to third parties.

14. These harms are independently actionable and justify the relief sought here, including statutory damages, actual damages, and restitution. In addition, because Defendants continue to collect sensitive consumer data without consent and have not changed their unfair and deceptive business practices, described herein, equitable relief, including an injunction, is appropriate here.

II. PARTIES

A. Plaintiffs

15. Patricia M. Cauley is a resident of Kendall Park, New Jersey. In January, 2017, Ms. Cauley purchased at a Best Buy store in Monmouth Junction, New Jersey a Samsung Smart TV, Model No. UN55KS8000FXZA.[6] At all times, Ms. Cauley used her Samsung Smart TV at her home in Kendall Park, New Jersey. Ms. Cauley connected her Samsung Smart TV to the Internet via a Wi-Fi connection shortly after purchasing it, and used "apps" like the Netflix, Hulu, and YouTube on the television to stream video content. She also uses her Smart TV to watch cable television and use other "smart" features.[7] Ms. Cauley's remote control for her Smart TV has a built-in microphone for voice recording. When Ms. Cauley purchased her Smart TV, she was not aware that Samsung would collect her personal and viewing data and/or the contents of her conversations and disseminate that information to third parties.

[6] A copy of Ms. Cauley's purchase receipt for her Samsung Smart TV at issue is attached hereto as Exhibit 2.

[7] A copy of the User Manual and Spec Sheet respecting Ms. Cauley's Samsung Smart TV at issue is attached hereto as Exhibit 3.

16. Plaintiff Thomas Roger White, Jr. is a resident and citizen of Miami Shores, Florida. During the Class Period, Mr. White purchased in Florida two Samsung Smart TVs (Samsung, Model No. UN55KU6300F, Serial No. 05HX3CAHB11790N and Samsung, Model No. UN32J5500AF, Serial No. 03NL3CGG90593M) and one Sony Smart TV (Sony, Model No. KDL-40W650D, Serial No. 5018352.), which are the subject of this dispute. Mr. White connected his Smart TVs to the Internet via a Wi-Fi connection shortly after purchasing it, and used "apps" like the Netflix, Hulu, and YouTube on the television to stream video content. He also uses his Smart TV to watch cable television, use other "smart" features, and play PlayStation and use a DVD player. When Mr. White purchased his Smart TVs, he was not aware that Samsung and/or Sony would collect his personal and viewing data and/or the contents of his conversations and disseminate that information to third parties.

17. When shopping for their Smart TVs, each Plaintiff looked at the description of the televisions provided on the boxes in which Defendants' Smart TVs were packaged. The packaging for the Defendants' Smart TVs described its features and indicated that the televisions were equipped to deliver video content through the Internet and could display content from cable and satellite providers, streaming devices, and other connected media sources. The packaging, however, failed to inform Plaintiffs that if they took advantage of those features or watched live broadcast programming on Defendants' Smart TVs, their personal and viewing data would be collected by Defendants and disseminated to third parties. It is also failed to inform Plaintiffs that if they took advantage of those features or watched live broadcast programming on Defendants' Smart TVs, the contents of their voice conversations would be analyzed and disclosed to third parties.

18. Had Plaintiffs known the truth about Defendants' collection and dissemination of Plaintiffs' personal and viewing data and voice recording practices, Plaintiffs would not have purchased, or would have paid substantially less for, Defendants' Smart TVs.

19. At no time did Plaintiffs consent to having their personal or viewing information or voice content collected and/or disseminated to third parties.

B. Defendants

20. Defendants are consumer electronics companies with corporate headquarters and contacts to New Jersey. Defendants sell millions of television and audio sets and other products in over 8,000 retail stores throughout the United States, including large chains such as Costco, Sam's Club, Walmart, and Best Buy.

21. Defendant Samsung Electronics America, Inc. ("Samsung") is headquartered at 105 Challenger Road Ridgefield Park, N.J. 07660, conducts substantial business in New Jersey; and is the market leader for HDTVs in the U.S. Defendant Samsung designs, markets, advertises, sells, and distributes for sale consumer electronic devices, including Smart TVs, throughout the United States and in this District. Defendant Samsung holds the largest market share of Smart TVs in the country.

22. Defendant Sony Electronics Inc. is a subsidiary of Sony Corporation, conducts substantial business in New Jersey and maintains its corporate campus at Sony Drive, Park Ridge, NJ 07656. Defendants, Inc. designs, markets, advertises, sells, and distributes for sale consumer electronic devices, including Smart TVs, throughout the United States and in this District.

III. JURISDICTION AND VENUE

23. This Court has jurisdiction over the subject matter of this action pursuant to U.S.C. § 1331, as this action arises under a federal statute. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

24. This Court also has jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because: (i) at least one Plaintiff is a citizen of a different state than the Defendants; (ii) the amount in controversy exceeds $5,000,000; and (iii) there are at least 100 individuals in the putative class that Plaintiffs seek to represent through this action.

25. This Court has personal jurisdiction over Defendants because Defendants regularly conduct business in New Jersey are present and licensed to conduct business in New Jersey, and because the events giving rise to this lawsuit occurred, in substantial part, in New Jersey.

26. Venue is proper in this District pursuant to 28 U.S.C. 1391(b) because Defendants are headquartered in this District, Defendants conduct substantial business in this District, and a substantial part of the events giving rise to Plaintiffs' claims occurred in this District. Plaintiff Patricia Cauley also resides in New Jersey and purchased and used her Smart TV in New Jersey, in this District. Venue also properly lies in this District because all Defendants conduct substantial business within this District, and because many of the Class Members reside in this district.

Application of New Jersey Law To
Consumers Nationwide is Appropriate

27. Each of the defendants are headquartered and/or have a substantial corporate presence in New Jersey and, upon information and belief, Defendants' United States sales strategy, advertising, marketing and product promotion was conceived in substantial part, and emanates from, Defendants' facilities in New Jersey.

28. Application of New Jersey law to consumers nationwide is appropriate because Defendants are headquartered here and/or maintain their US based corporate, marketing and advertising department(s) in New Jersey where the alleged misconduct, described herein, emanated from. In addition, Defendants' products are distributed throughout the United States to Plaintiffs and Class members located in New Jersey and/or distributed throughout the United States from fulfillment and other facilities located in New Jersey. New Jersey also has a substantial, compelling reason to protect consumers from deceptive and unlawful misconduct of companies with headquarters and a substantial presence there, and who regularly sell products in and/or from New Jersey.

IV. FACTUAL ALLEGATIONS

A. Smart TV Background

29. Concerns about the use of televisions to collect consumer information were anticipated in the 1980s.[8]

[8] 11 David A. Bode, Interactive Cable Television: Privacy Legislation, 19 Gonz. L. Rev. 725 (1984).

30. Privacy scholars and policy makers recognized the risk that interactive television would threaten the privacy of users if safeguards were not established.[9] These risks included the "danger similar to wiretapping," of "misuse and interception of 'private' information" during transmission to the central servers, as well as the insecurity of data once it arrived at the central servers.[10]

31. Since the mid-2000s, Smart TVs have become increasingly popular in the United States. A Smart TV is essentially a technological cross between a computer and a television. Aside from the traditional function of a television set, a Smart TV is also equipped with integrated software applications that allow users to access the Internet, and on-demand services such as Netflix, Hulu, and Pandora, and other online media content, such as Facebook and Twitter.

32. Although Smart TVs are more expensive than traditional television sets, Smart TVs are popular because they are equipped to deliver movies and television shows on an on-demand basis, including programming that may not be conventionally available (e.g., broadcast on network or cable television). Smart TVs thus bring the "video-store" into the home for users.

B. Defendants Begin Selling Smart TVs

33. Defendants bill themselves as leading high definition television producers in the United States. In addition to Smart TVs, Defendants manufacture and sell various audio and entertainment products. Defendants generate billions in revenue each year.[11]

[9] See William J. Broad, U.S. Counts on Computer Edge in Race for Advanced TV, N.Y. Times (Nov. 28, 1989), http://www.nytimes.com/1989/11/28/science/us-counts-o-computer-edge-in-the-race-for-advancedtv.html ("Finally, scientists say, the advent of digital television will aid the merging of computers and television, with the prospect of a rush of combined uses."); David Flaherty, Protecting Privacy in Two Way Electronic Services, Communications Library (1985).

[10] Bode, supra 13 at 711. See also *Cable Television Privacy Act: Protecting Privacy Interests from Emerging Cable TV Technology*, 35 Fed. Com. L.J. 71, 79 (1983).

[11] As of 2016, Smart TVs sales reached almost 250 million units. Sales are expected to grow to 330 million by 2019.

34. In or around January 2012, Defendants' began selling Smart TVs. Defendants' Smart TVs provide consumers with multiple access points to visual, audio, and other video content. Defendants' Smart TVs are further equipped with HDMI connections, coaxial connectors, analog audio outputs and inputs, and various video input connectors.[12]

35. Defendants' Smart TVs are also equipped with the ability to connect to the internet via wireless internet networking (hereinafter "WiFi"). Specifically, Defendants' Smart TVs allow consumers to access the WiFi networks to allow consumers to access and watch various forms of audio and visual entertainment online, as well as to find access to online news, weather, and entertainment sources.[13]

36. Defendants' Smart TVs are delivered to consumers with many pre-installed applications. These include such popular internet applications as Netflix, YouTube, Amazon, Pandora, HuluPlus, Twitter, and more. The list is ever-growing. Many of these applications stream video and other content to consumers via Defendants' Smart TVs.

37. Additionally, Defendants' Smart TVs provide access to cable television, satellite television, and on-demand viewing services. Such services also stream video and audio programming directly to Defendants' Smart TVs.[14]

C. *Defendants' Business Model*: Use Automatic Content Software To Secretly Spy On Consumers And Sell Their Personal Information For Profit

38. Defendants developed and use a business platform for the Smart-TV industry that rests on utilizing Automatic Content Software ("ACS") technology to capture, in real time, billions of viewing data points each day from millions of consumers' Smart TVs manufactured and sold by Defendants.

---

[12] See, e.g., Exhibit 3 attached hereto (User Manual and Spec Sheet respecting Ms. Cauley's Samsung Smart TV at issue).

[13] Id.

[14] Id.

39. Since 2012, Defendants have manufactured Smart TVs that continuously monitor and track, in real time, what consumers are watching, what consumers are saying, and the viewing habits of those consumers. Defendants then transmit this private, confidential information to Defendants' own servers – and sell this private, confidential information to third parties *without* first obtaining informed consent from the consumer.[15]

40. In other words, Defendants are secretly spying on its customers for profit. Defendants do not deny that they are violating its customers' privacy in this manner.

41. Defendants' ACS enables Defendants to monitor and identify Plaintiffs' and the Class Members' video viewing habits, personal information, and voice content.

42. Defendants' secretly provide this private, consumer information to third-party advertisers and content providers who, in turn, display targeted advertisements to consumers (based on consumers' data and information they have acquired from Defendants). In addition, Defendants and the third-party advertisers even place targeted ads on smartphones, tablets, PCs, or other devices within the home that share the same Internet connection as Defendants' Smart TV, and also within some Smart TV apps in Defendants' Smart TVs themselves.

43. Defendants tracking software captures (and Defendants then disclose) substantial, extensive information about Plaintiffs' and consumers' "*digital identities*;" namely, consumers' video-viewing history, consumers' computer addresses, and other confidential information about other devices connected to the same Wifi network.

44. Through Defendants' ACS, their Smart TVs are able to transmit information about what a consumer is watching on a second-by-second basis, in addition to the voice content of users. Defendants' tracking software captures information about a selection of pixels on the screen and sends that data to Defendants' servers, where it is matched up to

[15] See Consumer Reports, *Samsung, LG, and Vizio smart TVs are recording—and sharing data about—everything you watch, Consumer Reports investigates the information brokers who want to turn your viewing habits into cash*, February 27, 2015, http://www.consumerreports.org/cro/news/2015/02/samsung-lg-vizio-smart-tvs-watch-everything-you-watch/index.htm; The Verge, *Most smart TVs are tracking you – Vizio just got caught*, February 7, 2017, http://www.theverge.com/2017/2/7/14527360/vizio-smart-tv-tracking-settlement-disable-settings.

a database of *publicly available* television, movie, and commercial content. Defendants further collect viewing data from consumers' cable or broadband service providers, set-top boxes, external streaming devices, DVD players, and over-the-air broadcasts. Upon information and belief, Defendants store this data indefinitely.

45. Defendants' ACS software also periodically collects other information about the television, including IP address, wired and wireless MAC addresses, WiFi signal strength, nearby WiFi access points, and other items.

46. Defendants' ACS tracking software works by analyzing bits of the video and other visual programming its customers are watching, in real time. The technology then allows Defendants' to determine, amongst other information, the *date*, *time*, *channel of programs*, and *whether customers watched this programming in real time or from a recording.*[16]

47. Defendants' ACS tracking technology also allows Defendants to determine whether a viewer is watching a traditional television or cable program or whether the customer is viewing programming via streaming internet applications such as Netflix, Amazon Prime, or Hulu. The technology determines the time frame during which the programming was viewed, as well as the duration for which the customer actually viewed it.[17]

48. Defendants, armed with this surreptitiously-collected information on customers' viewing habits, then connect the information to the customers' personal internet protocol (hereinafter "IP") address. This is the internet address that is used to identify every internet connected device in a home, office, or other connected environment. These devices include smartphones, tablet computers, laptop computers, desktop computers, and any other wireless device that shares the same IP address as the Smart TV.

49. IP addresses are closely connected to the individuals using the specific

[16] See, e.g. Cognitive Network's Automatic Content Software Platform Diagram) (attached hereto as Exhibit 4).

[17] Id.

IP address. For instance, hundreds of personal attributes can be connected to a specific IP address, including a customers' age, profession, and certain wealth indicators.

50. ACS is also designed to scan a consumer's home WiFi networks to secretly collect information that is then utilized to help determine the specific person whose viewing activity has been collected. This allows Defendants to determine, within a certain degree of accuracy, which person in a home is watching what and when.

51. Defendants then sell consumer private information to third parties, including advertisers. Doing so allows advertisers and marketers to determine which advertisements to display on not only a consumer's Defendants' Smart TV, but also any other "smart" devices connected to the same IP address, such as smartphones, tablets, and computers.

52. Defendants provide consumers' data, voice content and other sensitive information to third parties for the purpose of targeting advertising to particular consumers on their other digital devices based on their television viewing data. Defendants earn substantial revenue by providing consumers' television viewing history to third parties through licensing agreements, on a television-by-television basis.

53. Defendants also facilitate the provision of demographic information about Smart TV users to third parties. Defendants disclose and use consumers' Internet Protocol (IP) addresses, media access control (MAC) addresses, zip codes and other information to identify a particular consumer or household, and then send third parties the demographic information associated with that consumer or household. Upon information and belief, Defendants' contracts with third-party users of the viewing data also allow the following information to be appended: sex, age, income, marital status, household size, education, home ownership, and household value. For all of these uses, Defendants provide highly-specific, second-by-second information about television viewing and other information, which allows third parties – and even an ordinary person – the ability to determine the consumers' electronic identity and location.[18]

[18] In this advanced technological-age, this data and other personally identifiable information disclosed by Defendants to third parties can easily be used by an ordinary person to pinpoint a consumer's physical

D. Defendants Collaborate With Cognitive Networks And Other Third Parties To Acquire and Sell Consumer Data

54. Defendants "partner[] with TV set manufacturers to enable content providers, advertisers, and others to provide greater engagement and interactivity to TV programming. [Third parties like] Cognitive Networks' ACR (automatic content recognition) platform makes Smart TVs aware of the programming that they are displaying, enabling transactions [and] informational requests . . . ." [19]

55. A Consumer Report investigation uncovered:

> Here's how it works: Companies such as Cognitive Networks, Enswers, and Gracenote collaborate with television manufacturers to embed [automatic tracking software] technology into smart TVs that monitors either the voice or audio stream – and sometimes both – that the user is watching. The [automatic tracking software] creates a "fingerprint" of the on-screen content, and then send it to a remote server that uses that fingerprint to determine what programming is being watched. Since much of the [automatic tracking software] process is handled by these third parties, *it is likely that millions of smart TV owners have inadvertently left an extensive data trail chronicling months, if not years, of their TV-watching history on the servers of companies they have never heard of*.[20]

---

location (i.e., "geolocation" information) and electronic identity. See, e.g., *How to Trace an IP Address to a PC & How to Find Your Own*, https://www.makeuseof.com/tag/how-to-trace-an-ip-address-how-to-find-your-own-nb/

[19] https://techcrunch.com/2015/01/04/cognitive-networks-ces/; https://www.crunchbase.com/orgaization/cgnitive-neworks. See also (Cognitive Network's Automatic Content Software Platform Diagram) (attached hereto as Exhibit 4).

[20] See Consumer Reports, *Samsung, LG, and Vizio smart TVs are recording—and sharing data about—everything you watch, Consumer Reports investigates the information brokers who want to turn your viewing habits into cash*, February 27, 2015, http://www.consumerreports.org/cro/news/2015/02/samsung-lg-vizio-smart-tvs-watch-everything-you-watch/index.htm (emphasis added).

56. Cognitive Networks has admitted using consumer information it has obtained from Defendants for advertising purposes.[21] In a 2013 press release, the company highlighted the value of ACS for advertisers, who could not otherwise "pinpoint what viewer's interests are and provide more targeted advertisements based on their preferences." In fact the market research firm for Cognitive Networks lists the "always on" nature of ACS as one of its key benefits, and claims: "The consumer does not need to opt-in to an app or service in order to interact with enhanced TV features."[22]

57. Enswers has admitted that, in 2012, its tracking software has been embedded at the hardware level into Samsung smart TVs. Enswers has already used the technology to push interactive advertisements for retirement-planning financial products in Spain, and also has prompted Samsung smart TV owners to purchase David Beckham underwear during the Super Bowl XLVIII using their remote controls.[23]

58. Defendant Samsung has also identified companies called "Nuance" and "Enswers" as some of the third parties it transmits consumers' information to.[24]

---

[21] As Zeev Neumeier, Cognitive Network's Founder and President, explained, the data recognition/processor, third-party companies like Cognitive Networks that Defendants employ to collect private confidential information and watching habits about consumer utilize:

> [A]utomatic content recognition (ACR) that looks at the picture on your TV and uses that data to identify exactly what you're watching. That, in turn, enables a content provider or advertiser to add interactive overlays to the TV screen itself, triggered by what's onscreen at the moment — say, a poll that's relevant to a scene in a show or a coupon that's tied to an ad.

https://techcrunch.com/2015/01/04/cognitive-networks-ces/. See also (Cognitive Network's Automatic Content Software Platform Diagram) (attached hereto as Exhibit 4).

[22] See Consumer Report, http://www.consumerreports.org/cro/news/2015/02/samsung-lg-vizio-smart-tvs-watch-everything-you-watch/index.htm.

[23] See Consumer Reports, *Samsung, LG, and Vizio smart TVs are recording—and sharing data about—everything you watch, Consumer Reports investigates the information brokers who want to turn your viewing habits into cash*, February 27, 2015, http://www.consumerreports.org/cro/news/2015/02/samsung-lg-vizio-smart-tvs-watch-everything-you-watch/index.htm

[24] Id.

E. Consumers Are Not Reasonably Informed By Defendants Of Their Tracking And Recording And Disclosure To Third Parties Of Consumers' Private Information

59. Consumers have no reason to expect that Defendants engaged in second-by-second tracking of consumer viewing data by surreptitiously decoding content and sending it back to their own servers, and then on to third parties' servers. Further, Defendants' representations were not sufficiently clear or prominent to alert consumers to their practices related to data collection and transmission.

60. Neither Defendants' Smart TV set up, nor Defendants' TV box, manual, spec sheet, advertising, or marketing specifically states that Defendants monitor, track, and report viewing habits and private information about devices attached to home networks, or that Defendants then transmit that information to third parties for profit. Nor do Defendants' proactively notify its consumers that the company will be collecting the consumers' viewing data by utilizing the pre-installed tracking software or the specific third-parties Defendants have contracts with. Rather, Defendants omit this material information in its communications with its consumers.

61. In reality, Defendants conceal their ACS and the method for disabling it. In order to not be subjected to Defendants ACS and monitoring programs forever, the consumer must somehow attempt (while taking the unit out of a cardboard box and attempting to physically install it or, as is often the case, having someone else set it up for the consumer) to:

a. find the privacy policy, read and comprehend the complex legal text;

b. understand how, why, when, and if Defendants are collecting confidential, personally identifiable information about them;

c. determine whether or not Defendants' data collection is for Defendants' profit;

d. figure out if Defendants are monitoring and collecting their personal information in real time;

e. try to compute how much information Defendants are collecting and from which devices; and

f. determine if Defendants are storing consumers' private information on their servers, and for how long.

62. Then, consumers must then attempt to figure out:

i. when and if Defendants are transmitting their information to outside third parties,

ii. how much information they are transmitting to third parties and for what purposes,

iii. to what third parties they are transmitting consumer information to, and what the privacy policies of the outside third parties are; and

iv. whether the third parties are storing consumers' private information on their servers, and for how long.

63. Consumers must further attempt figure out:

a. if those outside third parties are transmitting their personal information to other outside "second level" third parties, and

b. to what "second level" third parties Defendants are transmitting consumer information to;

c. how much information they are transmitting to "second level" third parties and for what purposes;

d. what the privacy policies of the outside "second level" third parties are; and

e. whether the "second level" third parties are storing consumers' private information on their servers, and for how long.

64. As a Consumer Reports investigation about Defendants' Smart TVs determined:

> [A] key concern with the user monitoring features now built into smart TVs: Consumers don't know precisely what they're enabling when they click through the TV's privacy policy. When Consumer Reports set up a current Samsung smart TV, we were confronted with a

> terms of service and privacy agreement that had *nine separate expandable sections to explore*. One section, the "Smart Hub Privacy Policy," *covered 47 screens' worth of text*. . . . Regardless, [] [Samsung Smart] TVs allow you to zip through these agreements by agreeing to them all at once. *And a consumer could hardly be blamed for not wanting to read thousands of words of legal documentation on their TVs when they're trying to set them up for the first time*.[25]

65. Furthermore, Defendants' customers do **not** have access to the names of the outside third parties (or outside "second level" third parties) or access to the separate privacy policies of these outside parties (or outside "second level" third parties) or access to the licensing agreements between Defendants and these third parties. Thus, for the vast majority of consumers who are unaware of the need to take steps to ensure their privacy, Defendants do nothing to alert them, preferring to keep their invasive monitoring and tracking practices – their "backdoor billion dollar business" -- a secret from its customers.

66. Further, even were a consumer to understand the privacy policy and the so called "option" to not be subjected to Defendants ACS and automatic monitoring programs, consumers are then unable to use some or most of the "Smart" features on their Smart TV -- the very reason consumers buy (and pay considerable extra) when purchasing Smart TVs in the first place.[26]

---

[25] See Consumer Reports, *Samsung, LG, and Vizio smart TVs are recording—and sharing data about—everything you watch, Consumer Reports investigates the information brokers who want to turn your viewing habits into cash*, February 27, 2015, http://www.consumerreports.org/cro/news/2015/02/samsung-lg-vizio-smart-tvs-watch-everything-you-watch/index.htm.

[26] See, e.g. TechDirt, *LG Will Take The Smart Out Of Your Smart TV If You Don't Agree To Share Your Viewing and Search Data With Third Parties*, May 20,2014, https://www.techdirt.com/articles/20140511/17430627199/lg-will-take-smart-out-your-smart-tv-if-you-dont-agree-to-share-your-viewing-search-data-with-third-parties.shtml; See also Slashdot, *Television Privacy Declining LG's New Ad-friendly Privacy Policy Removes Features From Smart TVs* ("Techdirt and Consumerist posted articles about a user . . . [who] declined their new [LG Smart TV] Privacy Policy, only to find that most Internet-connected features (e.g. BBC iPlayer, Skype) of the TV now no longer work."), May 21, 2014, https://entertainment.slashdot.org/story/14/05/21/1456206/declining-lgs-new-ad-friendly-privacy-policy-removes-features-from-smart-tvs.

67. As reported, Defendants' Smart TVs have continued to collect private information about consumers' even when consumers have successfully "opted out" of such monitoring.[27]

F. Defendants Know That Information They Disclose Identifies Individual Viewers, Their Viewing Habits, And Their Location

68. As discussed, consumers' private information that Defendants disclose to advertisers, data brokers, media content providers, and other third parties, such as its partners, includes viewing history and information which identifies individuals. This information reveals sensitive geolocation information and is personally identifying.

69. Media access control (MAC) addresses, for example, are unique 12-digit identifiers that are assigned to individual mobile devices, computers, Smart TVs, or other electronic devices. These addresses are tied to the devices' physical embedded chipsets and thus are persistent throughout the life of the device. MAC addresses are automatically broadcast when devices search for networks or communicate with other devices.

70. MAC addresses often can be linked to individuals by name. For example, when you sign into a commercial WiFi hotspot, your MAC address is tied to the information you use to sign up for the service. Additionally, automatic WiFi probes also broadcast the names of the last networks a device has connected to, which can reveal additional information about the individual, such as the name of a home or work network.

71. MAC addresses can be used to develop highly specific geolocation data. For example, retail analytics firms have used MAC addresses to pinpoint customer locations—a practice which the Federal Trade Commission ("FTC") has investigated.

72. When Defendants disclose MAC addresses of all the devices that connect to the same network as a Defendants Smart TV, along with IP addresses, zip codes, the online services consumers visit, the presence of other devices connected to the consumer's local

[27] See, e.g., NetworkWorld, *LG Smart TV spying, owner claims his USB filenames posted on LG servers*, Nov. 19, 2013, http://www.networkworld.com/article/2225848/microsoft-subnet/lg-smart-tv-spying--owner-claims-his-usb-filenames-posted-on-lg-servers.html.

network, the number of users and frequency of use of Defendants products and services, and other information, the disclosure provides a "game plan" to associate individuals with their viewing habits.

73. Defendants know that individuals and their viewing histories can be, and are easily being, identified and linked by the information Defendants disclose.

74. In fact, individuals can be identified with far less information than what Defendants disclose. A groundbreaking study published in 2000 revealed that three pieces of information—zip code, birth date (including year), and sex—uniquely identified 87 percent of the U.S. population.[28] Other studies have found similarly high rates of identification.[29]

75. At least since 2006, video service providers have known that the disclosure of viewing data not associated with individual names can nevertheless be associated with specific individuals. That year, Netflix released a data set representing the movies rated by over 480,000 Netflix customers and the date each rating was given. In an apparent effort by Netflix to anonymize the data, the company replaced customers' names with unique numbers and did not include addresses, phone numbers, or other direct identifiers.[30]

76. Netflix released the data "as part of its Netflix Prize contest, through which researchers competed to improve the algorithm Netflix uses to recommend movies to its subscribers. Netflix's algorithm takes into account past viewing habits and movie preferences of each of its subscribers."[31]

77. Following the release of this data set, two researchers at the University of

---

[28] Latanya Sweeney, *Uniqueness of Simple Demographics in the U.S. Population*, Carnegie Mellon University, School of Computer Science, Data Privacy Laboratory, Technical Report LIDAP-WP4 (2000).

[29] Philippe Golle, *Revisiting the Uniqueness of Simple Demographics in the US Population*, ACM Workshop on Privacy in the Elec. Society at 77, 78 (2006).

[30] March 12, 2010 Letter from Maneesha Mithal to Reed Freeman, https://www.ftc.gov/sites/default/files/documents/closing_letters/netflix-inc./100312netflixletter.pdf

[31] Id.

Texas announced that it was possible to identify a significant number of subscribers based on the data set released.[32] The researchers concluded -- **using 2008 technology**:

> We demonstrate that an adversary who knows only a little bit about an individual subscriber can easily identify this subscriber's record in the dataset. Using the Internet Movie Database as the source of background knowledge, we successfully identified the Netflix records of known users, uncovering their apparent political preferences and other potentially sensitive information. .. . . [Using publicly-available movie reviews posted by Netflix subscribers on the popular site IMDb (www.imdb.com)], one could determine all of the Netflix movies that a subscriber had rated for a given period of time.[33]

78. Defendants thus know that third parties to whom it discloses this information, which includes its partners, can and do connect these dots. And **using 2018 technology**, so can the ordinary person.[34] The linkage between viewing data and individuals is firm and readily foreseeable to Defendants, in particular because the information it discloses is effectively a correlated look-up table, complete with geolocation data.

G. Defendants' Product Packaging, Advertising, Marketing, And Website Are False And/Or Misleading And Omit Material Information

79. In advertising and marketing, and on product packaging, Defendants promotes the connectivity of its Smart TVs, but Defendants repeatedly fails to adequately inform consumers about its data collection program, including that viewing data and personally identifiable information is being disclosed to third parties. The information

[32] Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, Proceedings of the 2008 IEEE Symposium on Security and Privacy at 111-123, https://dl.acm.org/citation.cfm?id=1398064.

[33] Id. These researchers were able to identify one user's movie choices, which may suggest facts about his or her politics ("Fahrenheit 9/11"), religious views ("Jesus of Nazareth"), or sexual preference ("Queer as Folk").

[34] See, e.g., *How to Trace an IP Address to a PC & How to Find Your Own*, https://www.makeuseof.com/tag/how-to-trace-an-ip-address-how-to-find-your-own-nb/.

disclosed is valuable and useful precisely because it is not anonymous but instead is personally identifying. Defendants also do not properly disclose that it sells this information to third party advertisers and data brokers.

80. Defendants rather give consumers a false sense of security when it comes to privacy by saying nothing about its ACS technology, which it uses.

81. Even today, ACS technology is conspicuously absent from Defendants' online advertising for entire product lines, including Plaintiffs' Smart TVs at issue. Defendants' website and Smart TV manuals tout its Smart TVs connectivity but do not disclose that Defendants will collect and disseminate to third parties for profit viewing habits and personal information upon connection.[35]

H. Consumers Do Not Believe That Defendants' Voice Recognition Involves Voice Recording or Transmission

82. The Electronic Privacy Information Center ("EPIC"), a leading consumer group before the FTC, has filed an FTC privacy complaint against Defendant Samsung and deemed the type of conduct by Defendants alleged herein to be misleading and deceptive.[36] EPIC stated: "Samsung users could not reasonably have anticipated that by using a voice-controlled Smart TV, their private conversations would be transmitted, sometimes unencrypted, to a third party company," and has compiled many statements from consumers regarding the fact that they never knew (or could possibly imagine) that voice recognition system in Smart TVs could intercept and record private communications in the home, or that Defendants would transmit those private recordings to outside parties.[37]

---

[35] See, e.g., Exhibit 3 attached hereto (User Manual and Spec Sheet respecting Ms. Cauley's Samsung Smart TV at issue).

[36] See In re: Samsung Electronics Co., Ltd. 20 Federal Trade Commission, February 24, 2015 (the "FTC Samsung Brief") (attached hereto as Exhibit 5).

[37] The survey conducted by EPIC only concerned Samsung Smart TV users, but the confusion expressed there applies equally to both Defendants. Counsel for Plaintiffs is more than willing to perform similar surveys for Defendant Sony if the Court so desires.

83. For example, a Smart TV user Dane Jensen commented:

> This is an outrageous invasion of privacy and should be illegal. Actually it is illegal but not being enforced. You are not allowed to spy or record someone without consent. I just bought a Samsung TV and never saw or signed any consent form to be recorded. I never saw anything.[38]

84. User Stephen commented:

> This should have to be relayed to the customer prior to purchasing. Shame on Samsung for giving into the governments constant strive to monitor the entire population[39]

85. User potrzebie commented, "I own two Samsung TVs and a Samsung tablet. If they don't stop this right now, I will never buy another Samsung product, ever. Vote with your wallets people.[40]

86. Twitter user @Jason_Garber commented, "From now on wherever I have business meetings and there is a #Samsung #SmartTV present I will ask for its removal."[41]

87. Twitter user @CSElder commented, "@Samsungtweets i will NEVER buy another Samsung tv thanks to your recording feature. You overstep your bounds. #SamsungFail"[42]

88. User beverly commented, "why is this info sent to third party at all it should just stop at the smart tv processor" [43]

89. User cft6vgy7 commented,

> This is why devices like cameras and microphones should always be sold separately from computers, TVs, and other electronics. It may not be as "convenient" for the less tech-savvy, but it will be more secure for

[38] Id. at 7, 19.
[39] Id.
[40] Id.
[41] Id.
[42] Id.
[43] Id.

> every single consumer. Allow consumers to "opt-in" if they don't mind the security risk; don't force users to have to "opt-out" if they want to preserve their own privacy. [44]

99. User John Manso wrote,

> I'm glad this is getting national attention. When I first saw the smart TV's come out, very few were concerned. A device in your living room with a camera, a microphone, and 24 hour access to the internet. What could go wrong here? Uh, everything. Who knows who can hack into all of these with a simple piece of software. Everything can be "hacked". No we don't cook up
> national threats in our living room but privacy is expected and deserved in one's living room wouldn't you say?[45]

100. User Craig Cheatham commented:

> There are a couple problems evident here beside the obvious one of spying on our conversations. All of these User Agreements convey all sorts of rights to the company without articulating them in a clear manner to the consumer. . . . There is NO way to know what is "shared" or who has access to it. . . . This trope of Future Shock is a new societal psychological syndrome, as yet unnamed. It is not really paranoia, it is a response to the unwilling sharing of our personal lives that we are powerless to stop without becoming a tree dwelling Luddite. It is an intrusion into what had been considered private personal space.[46]

V. CLASS ACTION ALLEGATIONS

101. Pursuant to Rules 23(a), 23(b)(2), or 23(b)(3) of the Federal Rules of Civil Procedure, Plaintiffs bring this class action on behalf of themselves and all Members of the Nationwide Class (the "Nationwide Class"), which shall initially be defined as:

> *All individuals in the United States who purchased a Samsung and/or Sony Smart TV with content-recognition capability for personal or household use, and not for resale, during the applicable statute of limitations period.*

[44] Id. at 7-8.
[45] Id. at 8.
[46] Id.

102. Additionally, or in the alternative, pursuant to Rules 23(a), 23(b)(2), or 23(b)(3) of the Federal Rules of Civil Procedure, Plaintiffs bring this class action on behalf of themselves and all Members of the New Jersey Class (the "New Jersey Class"), which shall initially be defined as:

> *All persons in New Jersey who purchased a Samsung and/or Sony Smart TV with content-recognition capability for personal or household use, and not for resale, during the applicable statute of limitations period.*

103. Additionally, or in the alternative, pursuant to Rules 23(a), 23(b)(2), or 23(b)(3) of the Federal Rules of Civil Procedure, Plaintiffs bring this class action on behalf of themselves and all Members of the Florida Class (the "Florida Class"), which shall initially be defined as:

> *All persons in Florida who purchased a Samsung and/or Sony Smart TV with content-recognition capability for personal or household use, and not for resale, during the applicable statute of limitations period.*

104. Excluded from the Classes are governmental entities, Defendants, any entity In which Defendants have a controlling interest, and Defendants; officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns. Also excluded from the Classes are any judge, justice, or judicial officer presiding over this matter, and the members of their immediate families and judicial staff.

105. The Classes described in this Complaint may be jointly referred to as the "Class" and proposed Members of the Classes may be jointly referred to as "Class Members."

106. Plaintiffs reserve the right to amend or modify the Class and/or Subclass definitions with greater specificity, further division into subclasses, or with limitation to particular issues as discovery and the orders of this Court warrant.

107. The Court can define the Class and create additional subclasses as may be

necessary or desirable to adjudicate common issues and claims of the Class Members if, based on discovery of additional facts, the need arises.

108. Pursuant to Rule 23(b)(2) of the Federal Rules of Civil Procedure, Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making final injunctive relief or corresponding declaratory relief and damages appropriate with respect to the Class as a whole. Specifically, Defendants continue to obtain and disseminate sensitive viewing histories and personal information on an opt-in basis and without consent, and to date have not adequately disclosed the true nature of the Defendants Smart TVs with ACS tracking technology, including that the TVs collect and disseminate consumers' personal information and voice-content.

109. Numerosity and Ascertainability: The exact number of members of the Class is unknown as such information is unavailable to Plaintiffs at this time. However, Plaintiffs believe individual joinder in this case is impracticable. The Class likely consists of hundreds of thousands of individuals. These individuals can be readily ascertainable through Defendants or their agents' records and are obtainable to Plaintiffs only through the discovery process.

110. Predominance of Common Questions of Fact and Law: Questions of law and fact common to all Class members exist and predominate over any questions affecting only individual Class members, including, but not limited to, the following:

a. Whether Defendants unlawfully collected and disseminated Plaintiffs' and Class members' personal information;

b. Whether Defendants disclosed to Plaintiffs and Class members before the tracking software was activated on Defendants' Smart TVs that their personal information would be collected and disseminated to third parties;

c. Whether Defendants misrepresented or omitted material facts with regard to the ACS feature of Defendants' Smart TVs;

d. Whether Plaintiffs and Class members consented to the collection of their personal information and its sale to third parties;

e. Whether Plaintiffs and Class members have a reasonable expectation of privacy in the information collected and disseminated by Defendants;

f. Whether Defendants' conduct constitutes violations of the laws and statutes asserted herein;

g. Whether Defendants' conduct was knowing;

h. Whether, as a result of Defendants' conduct, Plaintiff and Class members are entitled to damages, including compensatory, statutory, or punitive, and the amount of such damages;

i. Whether, as a result of Defendants' conduct, Plaintiffs and Class members are entitled to equitable relief, such as declaratory or injunctive relief;

j. Whether Defendants were unjustly enriched by their conduct;

k. Whether, for the Nationwide Class noted above, New Jersey has a significant contact to the claims of each class member to apply New Jersey law to all members of the Nationwide Class;

l. Whether, for the Nationwide Class noted above, the Video Privacy Protection Act and/or the Wiretap Act applies to all members of the Nationwide Class; and

m. Whether, as a result of Defendants' conduct, Plaintiff and Class members are entitled to an award of reasonable attorneys' fees, prejudgment interest, or costs of suit.

111. Typicality: Plaintiffs' claims, and Defendants' defenses, are typical of the claims and defenses of and to the Class. Every member of the Class was similarly affected by Defendants' course of conduct and experienced the same harm, damages and loss based on Defendants' unlawful conduct. As such, Plaintiffs and Class members must establish the same facts in order to prove the claims asserted herein.

112. Adequacy of Representation: Plaintiffs do not have any conflicts with any other members of the Class, and will fairly and adequately represent and protect the interests of the members of the Class and any other subclass. Plaintiffs have retained counsel competent and experienced in consumer protection and class action litigation, trials, and appeals.

113. Superiority of a Class Action: A class action is superior to other available methods for fair and efficient adjudication of this controversy. The expense and burden of the individual litigation would make it impracticable or impossible for the Class members to prosecute their claims individually. Absent a class action, Defendants likely will retain the benefits of its wrongdoing. Because of the small size of the individual Class members' claims, few, if any, Class members could afford to seek legal redress for these wrongs. Absent a representative action, the Class members will continue to suffer losses and Defendants will be allowed to continue these violations of law and to retain the proceeds of its ill-gotten gains. The trial and litigation of Plaintiffs' and Class members' claims are manageable. Individual litigation of the legal and factual issues raised by Defendants' conduct would increase delay and expense to all parties and the court system. The class action device presents far fewer management difficulties and provides the benefits of a single, uniform court judgment. Thus, the benefits of proceeding as a class action outweigh the difficulties.

VI. CAUSES OF ACTION

FIRST CLAIM FOR RELIEF

Unfair and Deceptive Tracking and Transmission - Violations of the NJCFA

(On Behalf Of Plaintiffs And The Nationwide Class, And Separately, On Behalf Of Plaintiff Cauley The New Jersey Class)

114. Plaintiff incorporates by reference each preceding and succeeding paragraph as though fully set forth at length herein.

115. Plaintiff brings this cause of action on behalf of himself and on behalf of all other members of the Class.

116. The CFA, N.J. Stat. Ann. § 56:8-2, prohibits:

> The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression, or omission of any material fact with intent that others rely upon such concealment,

> suppression or omission, in connection with the sale or advertisement of any merchandise . . . .

117. The CFA defines "merchandise" as "any objects, wares, goods commodities, services or anything offered, directly or indirectly to the public for sale." N.J. Stat. Ann. § 56:8-1(c).

118. At all relevant times, Defendants have engaged in the advertisement, offering for sale and sale of merchandise within the meaning of N.J. Stat. Ann. § 56:8-1(c), specifically Defendants' Smart TVs and related services.

119. Defendants use ACS technology to comprehensively collect the sensitive television viewing activity of consumers or households across cable or broadband services, set-top boxes, external streaming devices, DVD players, and over-the-air broadcasts, on a second-by-second basis and store this viewing data indefinitely.

120. Defendants provided this viewing data to third parties, which used it to track and target advertising to individual consumers across devices. Defendants engaged in these practices through a medium that consumers would not expect to be used for tracking, without consumers' consent; namely, consumers' own Smart TVs.

121. As described herein, Defendants' continued utilization of unlawful and unconscionable marketing practices, and their continuing practice of monitoring, tracking, and reporting viewing habits and personally identifiable information to unauthorized third parties, without consent, constitutes a deceptive act or practice in violation of the CFA.

122. Further, such is also an unconscionable commercial practice in violation of the CFA. Each instance of Defendants' unfair tracking constitutes a separate violation under the CFA, N.J. Stat. Ann. § 56:8-2.

123. The disclosure of personal viewing history, spending and watching habits, personal voice content, and personally-identifiable information is a material term of the transactions at issue as it is likely to affect a consumer's choice of, or conduct regarding, whether to purchase a product or service. The failure to inform consumers that this personal information would be shared with third parties is materially misleading.

124. Defendants' omission of this information was an act likely to mislead Plaintiff and the Class acting reasonably under the circumstances and constitutes a deceptive trade practice in violation of the CFA.

125. Defendants conduct was deceptive and unconscionable because, among other misconduct described in this Complaint, Defendants monitored, tracked, recorded and transmitted to third parties Plaintiffs' and Class members' personal viewing and spending habits and personally identifiable information without providing clear and conspicuous notice and without consent.

126. Defendants' collection and sharing of confidential sensitive data and voice content without consumers' consent has caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves.

127. This is an unfair act or practice, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

128. Defendants' practice of monitoring, tracking, and transmitting to third parties Plaintiffs' and Class members' personal viewing and spending habits and personally identifiable information and voice content without providing clear and conspicuous notice and without consent is also unlawful, deceptive and misleading, and violates the Wiretap Act, 18 U.S.C. § 2510 et seq., and Video Privacy Protection Act, 18 U.S.C. §§ 2710 et seq.

129. Defendants violations of these statutes constitute additional violations by Defendants of the CFA.

SECOND CLAIM FOR RELIEF

Deceptive Omissions - Violations of the NJCFA

(On Behalf Of Plaintiffs And The Nationwide Class, And Separately, On Behalf Of Plaintiff Cauley The New Jersey Class)

130. Plaintiffs incorporate by reference all the foregoing paragraphs.

131. Defendants engaged in deceptive practices as defined under the CFA. Defendants' actions were part of a scheme intended to actively mislead Plaintiffs and the Class into believing that the Smart TVs were of a specific quality, namely that the Smart TVs would not violate their privacy and were not designed to violate consumer's privacy by secretly monitoring and recording consumers' viewing habits, while Defendants did in fact know that their Smart TVs were designed to accomplish precisely this objective.

132. Additionally, Defendants did not disclose that their tracking software was installed and/or used on the Smart TVs because they knew that Plaintiffs and the members of the Class would not likely purchase the Smart TVs if they knew of the tracking software.

133. Defendants also made material omissions when speaking to Plaintiffs and Class Members through written materials. As described fully above, Defendants failed to clearly and conspicuously inform consumers that once their Smart TVs were hooked up to the internet through an IP address, Defendants would monitor, track, and transmit personal viewing histories and personally-identifiable information and voice content to third parties without Plaintiffs' and Class Members' consent.

134. Defendants failed to clearly and conspicuously inform Plaintiffs that once their Smart TV were hooked up to the internet through an IP address, Defendants would monitor and track their and their family's personal viewing histories and personally-identifiable information, and then transmit that confidential information and voice content to third parties without Plaintiffs' consent.

135. Defendants also failed to adequately disclose that the ACS feature of their Smart TVs comprehensively collected and shared consumers' television viewing activity from cable boxes, DVRs, streaming devices, and airwaves, which Defendants then provided on a household-by-household basis to third parties (and then to "second-level" third parties) .

136. Defendants' deceptive acts and practices were capable of deceiving a

substantial portion of the purchasing public. In fact, the Defendants knew and intended that Plaintiffs and the Class could not be expected to learn about or discover the existence of the Automatic Content Software on the Defendants' Smart TVs.

137. Through these deliberate omissions, the Defendants deceived the Plaintiffs about the quality of the Defendants Smart TVs and, as such, wrongfully induced Plaintiffs to purchase the Smart TVs.

138. The relationship between Defendants and Plaintiffs and the Class gave rise to the duty to speak because Defendants knew that their Smart TVs would, once connected to the internet, obtain confidential information about consumers, including viewing histories and personally identifiable information, and transmit that information to third parties without the knowledge or consent of the viewer. Defendants had superior knowledge as to the information withheld, and such information was material.

139. By engaging in the deceptive conduct, Defendants obtained substantial financial benefits by selling information about the Plaintiffs and the Class, including personally identifiable information, to unauthorized third parties.

140. The injuries caused by the Defendants' conduct are not outweighed by any countervailing benefits to consumers or competition, and neither Plaintiff nor the Class could have reasonably avoided the injuries they sustained.

141. Defendants intended that Plaintiffs and the Class would rely upon Defendants' deceptive conduct and not be aware of or understand Defendants' Automatic Content software.

142. The acts complained of herein, and each of them, constitute unfair, unlawful or fraudulent business acts or practices in violation of the CFA. Such acts and practices have not abated and will continue to occur unless enjoined.

143. The unfair, unlawful, or fraudulent business acts or practices set forth above have and continue to injure Plaintiffs, the Class, and the general public and cause the loss of money. These violations have unjustly enriched Defendants at the

expense of Plaintiffs and the Class.

144. The unfair, unlawful, or fraudulent business acts or practices at issue in this Complaint and carried out by Defendants took place in the course of trade or commerce.

145. As a direct and proximate result of Defendants' violations of the CFA, Plaintiff and the Class have suffered harm in the form of paying monies to purchase the Smart TV when they would not have otherwise.

146. Defendants' failure to adequately disclose its practice of secretly monitoring and tracking consumers and then and then transmitting that private, sensitive data and information and voice content to third parties, and other misconduct by Defendants (described herein), also constitute unconscionable commercial practices in violation of the CFA. Each separate instance of Defendants' failure to adequately disclose its practice of secretly monitoring and tracking consumers and then transmitting that private, sensitive data and information and voice content to third parties, and other misconduct by Defendants, constitutes a separate violation under the CFA, N.J. Stat. Ann. § 56:8-2.

THIRD CLAIM FOR RELIEF

Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710

(On Behalf of All Plaintiffs and the Nationwide Class Against All Defendants)

147. Plaintiffs incorporate by reference the foregoing allegations as if fully set forth herein.

148. Defendants are each a video tape service provider subject to 18 U.S.C. § 2710(a)(4) of the Video Privacy Protection Act ("VPPA"). Defendants are "engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials" by delivering videos to consumers through its Internet-connected Smart TVs. Defendants facilitates the transmission of specific video titles to be made to consumers through its video services that

allow consumers to watch movies and TV shows, listen to music, and access applications on demand.

149. As users of Defendants' Smart TVs, Plaintiffs and members of the Class are consumers within the definition of 18 U.S.C. § 2710(a)(1) of the VPPA.

150. Plaintiffs and the members of the Class have watched many movies and television shows on the Defendants' Smart TVs. At all times during the Class Period, Defendants' secretly monitored Plaintiffs' and Class members'' usage of their Smart TVs, collected information on Plaintiffs' and Class members' viewing habits, and performed scans of Plaintiffs' and Class members' home WiFi.

151. Unbeknownst to Plaintiffs and members of the Class, Defendants have disclosed and continue to disclose Plaintiffs' and the Class members' information, including their personally identifying information, to unidentified, unauthorized third parties.

152. Defendants' transmissions of Plaintiffs' and the Class members' personally identifiable information to these third party brokers and advertisers constitutes "knowing[] disclosures" of Plaintiffs' and the Class members' "personally identifiable information" to a person under the VPAA. 18 U.S.C. § 2710(a)(1).

153. The collection of consumers' viewing information – including movies, shows, and programs viewed, IP addresses, media access control (MAC) addresses, zip codes, computer names, and product serial numbers – constitutes the collection of personally identifiable information ("PII") within 18 U.S.C. § 2710(a)(3), because it "includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."

154. Defendants have disclosed, and continues to disclose, PII to third-parties, including data brokers and advertisers, to generate revenue and profit. 1

155. Defendants failed to solicit and/or obtain consent from Plaintiffs and the Class Members to collect and disclose their PII, nor did Defendants provide clear and conspicuous notice of the disclosure of PII, as defined in 18 U.S.C. § 2710 (b)(2)(B).

156. Defendants' disclosures were not made in the ordinary course of business as

defined by 18 U.S.C. § 2710(a)(2), which limits disclosures to "debt collection activities, order fulfillment, request processing, and the transfer of ownership."

157. Defendants are "video tape service providers" as defined by the VPPA. Defendants "engage[s] in the business, in or affecting interstate or foreign commerce, of rental, sale or deliver of prerecorded video cassette tapes *or similar audio visual materials*." 18 U.S.C. § 2710(a)(4). Specifically, Defendants deliver videos and "similar audio visual materials" to consumers through its internet-connected Smart TVs, as well as through many of the pre-loaded applications available on its Smart TVs.

158. Plaintiffs are considered "consumers" under the VPPA because they are each a "renter, purchaser or subscriber of goods or services from a video tape service provider[.]" 18 U.S.C. § 2710(a)(1). As described above, Plaintiffs and the Class caused to be purchased Smart TVs manufactured, marketed, and distributed by Defendants.

159. The knowing disclosure and transmission of PII by Defendants violates the VPPA within the meaning of 18 U.S.C § 2710(b)(1).

160. Accordingly, Plaintiffs and members of the Class are entitled under 18 U.S.C. § 2710(c)(2) to an award of damages (actual, liquidated, or punitive), reasonable attorneys' fees, other litigation costs reasonably incurred, and such other preliminary and equitable relief as the Court deems appropriate.

FOURTH CLAIM FOR RELIEF

Violation of the Wiretap Act, 18 U.S.C. § 2510 et seq.

(On Behalf of All Plaintiffs and the Nationwide Class Against All Defendants)

161. Plaintiffs reallege and incorporate by reference all of the preceding paragraphs.

162. The Federal Wiretap Act, 18 U.S.C. § 2510 et seq., prohibits the interception of any wire, oral, or electronic communications. The statute confers a civil cause of action on "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

163. "Electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce…" 18 U.S.C. § 2510(12).

164. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

163. "Contents" is defined as "includ[ing] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

165. "Person" is defined as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6). Plaintiffs and Class members are persons as defined under § 2510(6) of the Act.

166. Defendants' automated content software technology, which is installed and/or used by Defendants on their Smart TVs, is a device for purposes of the Wiretap Act because it is software used to intercept electronic communication.

167. Defendants, through their design, authorship, programming, knowing and intentional installation, activation, and/or other involvement with ACS software have intentionally intercepted, endeavored to intercept, and/or procured others to intercept or endeavor to intercept, electronic communications as described herein, in violation of 18 U.S.C. § 2511(1)(a). This interception was acquired during transmission, Defendants' ACS operated in real time to acquire the content of Plaintiffs' and the Class members' electronic communications, including their viewing habits and identifying information, as described above.

168. The contents intercepted include information concerning the substance, purport, or meaning of that communication, including, but not limited to, viewing histories and preferences, IP addresses, MAC addresses, zip codes, product model numbers, hardware and software versions, chipset IDs, and region and language settings.

169. Plaintiffs' and the Class members' electronic communications were intercepted without their consent and for the unlawful and/or wrongful purpose of monetizing their private information, including by using their private information to create targeted advertisements for profit, without Class members' consent, and for tortious purposes and for the purpose of committing unfair business practices.

170. Defendants violated 18 U.S.C. § 2511(1)(d) by intentionally using or endeavoring to use, the contents of Plaintiffs' and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiffs' and Class Members' electronic communications.

171. Neither Plaintiffs nor Class Members authorized or consented to Defendants interception of electronic communications.

172. As a result, Plaintiffs and Class members have suffered harm and injury, including due to the interception and transmission of private and personal, confidential, and sensitive communications, content, and data.

173. Plaintiffs and the Class have been damaged by the interception or disclosure of their communications in violation of the Wiretap Act, as described herein, and are thus entitled to preliminary, equitable, or declaratory relief; statutory and punitive damages; and reasonable attorney's fees and litigations costs reasonably incurred. 18 U.S.C. § 2520(b).

174. 18 U.S.C. § 2520 also provides for a private cause of action and allows for declaratory and equitable relief as appropriate, damages, disgorgement of profits, and statutory damages of the greater of $10,000 or $100 a day for each day of violation, actual and punitive damages, and reasonable attorney's fees and costs.

FIFTH CLAIM FOR RELIEF

Violation of Florida's Deceptive And Unfair Trade Practices Act ("FDUTPA")
Fla. Stat. § 501.201, et seq.

(On Behalf Of Plaintiff White and The Florida Class)

175. Plaintiffs incorporate by reference the foregoing allegations as if fully set forth herein.

176. Plaintiffs and each member of the Class are "consumers" as defined by Fla. Stat. § 501.203(7).

177. Defendants, through their conduct alleged herein, are engaged in "trade or commerce" as defined by Fla. Stat. § 501.203(8).

178. The FDUTPA was enacted to protect consumers and businesses from unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce.

179. To this end, the FDUTPA declares as unlawful all unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce.

180. Defendants violated the FDUTPA because their conduct, as alleged herein, is deceptive and unfair.

181. Defendants' conduct is deceptive because it is likely to mislead a reasonable Consumer.

182. The specifications of a consumer product are a material term of any transaction in that they directly affect a consumer's choice and conduct in purchasing a product.

183. Despite the importance of specifications to consumer purchase decisions, Defendants do not disclose that their Smart TVs have the tracking software installed, and that the tracking software monitors, collects and disseminates consumer data.

184. On the boxes in which the Smart TVs were packaged, Defendants informed Plaintiffs that one would be able to stream and view video content from the Smart TVs, as well as connect the Smart TVs to other devices such as Blu-ray DVD players and gaming consoles. However, Defendants failed to inform Plaintiffs that if they take advantage of these features and/or watch live broadcast programming on their Smart TVs, their viewing data and voice content is collected and disseminated to third parties. Had Plaintiffs known the full truth about Defendants' collection and dissemination of Defendants' viewing data, Plaintiffs would not have purchased or would have paid less for their Smart TVs.

185. Defendants' failure to disclose these specifications of their Smart TVs, as well as Defendants' failure to gain consumer consent to allow Defendants to monitor and collect consumer information by use of the tracking software, deceived consumers into believing they were purchasing a benign entertainment device.

186. Had Defendants disclosed to consumers that their Smart TVs employed the tracking software, and that consumer viewing habits and other information would be collected and disseminated without consent or knowledge, consumers would not have bought, or would have paid less for, Defendants' Smart TVs and would have avoided Defendants' products and data practices.

187. In fact, Defendants did not disclose facts about the tracking software to consumers that purchased the Smart TVs because they knew consumers, acting reasonably under the circumstances, would not purchase, or would pay less for, the Smart TVs if the fact that tracking software was installed on the Smart TVs was disclosed prior to purchase.

188. Defendants' conduct is unfair because it offends established public policy and is immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers.

189. Defendants' conduct offends established public policy because it violated 18 U.S.C. § 2710 and 18 U.S.C. § 2510 et seq., as explained above.

190. Defendants' conduct is substantially injurious, and is immoral, unethical, oppressive and unscrupulous because Defendants monitor, collect, and record consumer viewing habits and other information in order to sell it to third parties for profit, and does so without disclosing its data practices to consumers or obtaining consumer consent for the collection and sale of consumer data.

191. Had consumers known Defendants' Smart TVs employed software that monitored, collected and disseminated consumer viewing habits and other data, consumers would not have purchased, or would have paid less for, Defendants' Smart TVs.

192. Moreover, by surreptitiously monitoring, collecting, and recording consumer viewing habits and other information, and by selling, or otherwise disclosing, that information to third parties without consumer knowledge or consent, Defendants prevent consumers from avoiding its data practices and from protecting their right to privacy and their right to control the dissemination of their personal information.

193. Defendants knew or had reason to know that Plaintiffs and the Class could not have reasonably known or discovered the existence of the tracking software, without disclosure by Defendants.

194. The injury to consumer privacy rights, and the causing of consumers to buy products they otherwise would have avoided, outweighs the profit motive and ultimate goal for Defendants' unauthorized and secretive monitoring, collection and dissemination of consumer data.

195. Defendants' deceptive and unfair conduct occurred during the marketing, distribution, and sale of Smart TVs, and therefore occurred in the course of Defendants' business practices.

196. Defendants' conduct directly and proximately caused Plaintiffs and the Class actual monetary damages in the form of the price paid for the Smart TVs.

197. If Defendants had disclosed that their tracking software was installed and

operating on the Defendants Smart TVs, Plaintiffs and Class members would not have purchased, or would have paid less for, the Smart TVs.

198. Pursuant to Fla. Stat. § 501.211, Plaintiffs seek an order (1) requiring Defendants to cease the deceptive and unfair practices described herein; (2) requiring Defendants to pay damages to Plaintiffs and the Class; and (3) awarding attorney's fees and court costs.

SIXTH CLAIM FOR RELIEF

Negligent Misrepresentation/Omission

(On Behalf of Plaintiffs Cauley and White, and the New Jersey and Subclasses)

199. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

200. Defendants negligently concealed, suppressed, or omitted a material fact. To wit, Defendants concealed the existence of their Smart TV tracking (ACS) software that tracks and collects the users' information and viewing history as well as information from other devices that are connected to the user's Wi-Fi network and its disclosure of such viewing history, along with other personally identifiable information.

201. Defendants were under a duty to Plaintiff and Class members to disclose that the Smart TVs contained the pre-enabled tracking software and that it disseminated such data due to the following reasons:

a. Defendants, as the manufacturers, were in a superior position to know of the existence of the pre-enabled tracking software and the dissemination of data on Defendants' Smart TVs;

b. The Video Protection Privacy Act prohibits the collection, interception, disclosure, and/or transmission of the information at issue without the prior, informed consent of Plaintiff and the Class members or the opportunity, given in a clear and conspicuous manner, to prohibit the disclosure;

c. Plaintiff and Class members could not reasonably have been expected to learn or discover that Defendants included pre-enabled tracking software on the Smart TVs, including the dissemination of such data;

d. Defendants should have known that Plaintiff and Class members could not reasonably have been expected to learn or discover that Defendants included pre-enabled tracking software on its TVs, and in fact, Defendants took steps to actively conceal the tracking software; and

e. Defendants should have known that the existence and nature of the pre-enabled software was a material fact that influenced the purchasing decision of Plaintiff and Class members.

202. Defendants negligently concealed and/or suppressed information about the tracking software and the dissemination of data collected by that software and other software. Defendants should have known that Plaintiff and Class members would not have purchased the Smart TVs for the price they paid if Defendants had disclosed the existence of pre-enabled tracking software.

203. Defendants recognized the materiality of the tracking software and its ability to profit from the sale of users' personally identifiable information to third parties

204. Plaintiff and Class members were unaware of the existence of the tracking software on Defendants' Smart TVs at the time of the purchases, along with the dissemination of data by that software and other software. Had they known, Plaintiff and Class members would not have purchased Defendants Smart TVs or would have paid less for them.

205. Defendants' conduct directly and proximately caused Plaintiff and Class members actual monetary damages in the form of the purchase price of the Smart TVs and damages as a result of the unauthorized access.

206. On behalf themselves and the Class, Plaintiffs seeks damages, including expenses, attorneys' fees, and costs, as a result of Defendants' negligence.

VII. PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all others similarly situated, respectfully request that this Court:

a. Determine that this action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs are proper class representatives, and appoint Plaintiffs' Counsel as counsel for the Class;

b. Enter an order declaring Defendants' actions are unlawful;

c. Award Plaintiffs and class members appropriate relief, including actual, statutory, and punitive damages;

d. Award Plaintiffs and class members restitution, disgorgement, and other equitable relief as the Court deems proper;

e. Award injunctive and declaratory relief as may be appropriate;

f. Award attorneys' fees and all other costs of prosecuting this action;

g. Award Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and

h. Grant additional legal or equitable relief as this Court may find just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

Dated: October 29, 2019

By: /s/ Mack Press

Mack Press, Esq.
BERMAN CLASS LAW
18 Watergate Lane
Patchogue, NY 11772
Mack@MackPress.com
516-330-7213